UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/640,453	08/17/2000	William C. Arnold	YOR9-2000-0331	4496

29683 7590 08/09/2004

HARRINGTON & SMITH, LLP
4 RESEARCH DRIVE
SHELTON, CT 06484-6212

EXAMINER	
NORRIS, TREMAYNE M	

ART UNIT	PAPER NUMBER
2137	7

DATE MAILED: 08/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/640,453	**Applicant(s)** ARNOLD ET AL.	
	Examiner Tremayne M. Norris	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 August 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to claims1-46 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1,2,4-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chi (US pat 5,978,917), and further in view of McLain (US pat 5,812,826).

Regarding claim 1, Chi teaches a system for monitoring operation of a software program in a network environment, comprising:

an execution component for executing the software program (col.4 lines 64-66),

a monitoring component for obtaining information about actions performed by the software program (col.4 lines 50-55); and a network emulation component, coupled to the network, for emulating the behavior of at least a host providing network services (col.4 lines 45-66); wherein

said execution component and said network emulation component cooperate with the network in order to elicit a behavior of the software program that is detectable by said monitoring component (col.4 lines 45-66).

Chi does not teach said execution component being coupled to an isolated network that does not have a direct connection to another network that is not an isolated network. McLain teaches said execution component being coupled to an isolated network that does not have a direct connection to another network that is not an isolated network (col.3 lines 11-18). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Chi's system for the detection and elimination of macro viruses with McLain's method for emulating network monitoring devices in order to allow realistic monitoring and control systems testing prior to actual implementation (McLain col.2 lines 53-65).

Regarding claim 2, Chi and McLain teach a system as in claim 1, in addition Chi teaches said emulation component further comprises a server programmed so as to return emulated results in response to a request resulting from the software program being executed on said execution component (col.4 lines 45-66).

Regarding claim 4, Chi and McLain teach a system as in claim 1, in addition Chi teaches where at least one of said emulation component and monitoring component are programmed so as to provide information about the performance of the software program for the purposes of testing, debugging, performance profiling, or optimization (col.4 lines 45-66).

Regarding claim 5, Chi and McLain teaches a system as in claim 1, in addition Chi teaches where at least one of said emulation component and monitoring component are programmed so as to provide information about actions of the software program for the purposes of reverse engineering or otherwise determining the function and behavior of the software program (col.4 lines 45-66).

Regarding claim 6, Chi and McLain teach a system as in claim 1, in addition Chi teaches where at least one of said emulation component and monitoring component are programmed so as to provide information about actions of the software program for the purposes of detecting a presence of an undesirable software entity within the software program (col.4 lines 45-66).

Regarding claim 7, Chi and McLain teach a system as in claim 6, in addition Chi teaches wherein the undesirable software entity comprises at least one of a worm or a virus (col.4 lines 45-66).

Regarding claim 8, Chi and McLain teach a system as in claim 6, in addition Chi teaches wherein the undesirable software entity comprises a worm that exhibits viral characteristics (col.4 lines 45-66).

Regarding claim 9, Chi and McLain teach a system as in claim 1, in addition Chi teaches where the elicited behavior of the software program comprises self-replication (col.2 lines 34-35).

Regarding claim 10, Chi and McLain teach a system as in claim 1, in addition Chi teaches the elicited behavior of the software program comprises viral or malicious activity (col.4 lines 45-66).

Regarding claim 11, Chi and McLain teach a system as in claim 2, in addition Chi teaches said server is programmed to determine what result to return based at least in part on a result of a corresponding real query sent to a corresponding real server on a corresponding real, non-isolated network (col.4 lines 45-66).

Regarding claim 12, Chi and McLain teach a system as in claim 2, in addition Chi teaches said server is programmed so as to function as an optimistic host (col.4 lines 45-66; col.5 lines 15-20).

Regarding claim 13, Chi and McLain teach a system as in claim 2, in addition Chi teaches where said server comprises at least one of a real or an emulated Web server (col.4 lines 45-48).

Regarding claim 14, Chi and McLain teach a system as in claim 2, but do not teach said server comprises at least one of a real or emulated http, ftp, imap4, pop3, nntp, news, irc, chat, smtp, mail and mailbox server. Examiner takes official notice that http, ftp, imap4, pop3, nntp, news, irc, chat, smtp, mail and mailbox servers are well known in the art. It would have been obvious to one of ordinary skill in the art to use one of these servers in order to obtain efficient network communication.

Regarding claim 15, Chi and McLain teach a system as in claim 2, but do not teach a real or emulated router. Examiner takes official notice that routers used in conjunction with servers are well know in the art. It would have been obvious to one of ordinary skill to use a router with a server in order to expedite message delivery.

Regarding claim 16, Chi and McLain teach a system as in claim 2, but do not teach said server comprises at least one of a real or emulated DNS, WINS, or other Name server. Examiner takes official notice that DNS, WINS, or other Name servers are well known in the art. It would have been obvious to one of ordinary skill in the art to use one of these servers in order to associate a computer's host name with its address.

Regarding claim 17, Chi and McLain teach a system as in claim 2, but do not teach said server comprises at least one of a real or emulated SNMP server. Examiner takes official notice that SNMP servers are well known in the art. It would have been obvious to one of ordinary skill in the art to use SNMP in order to be able to monitor the activity in the various devices on the network and report to the network console workstation.

Regarding claim 18, Chi and McLain teach a system as in claim 2, but do not teach said server comprises at least one of a real or emulated NetBIOS server. Examiner takes official notice that NetBIOS servers are well known in the art. It would have been obvious to one of ordinary skill in the art to use NetBIOS servers in order to provide application programs with a uniform set of commands for requesting the lower-level network services required to conduct sessions between nodes on a network and to transmit information back and forth.

Regarding claim 19, Chi and McLain teach a system as in claim 2, but do not teach said server comprises at least one of a real or emulated server that operates in accordance with SMB, NES or other distributed file system protocols. Examiner takes official notice that SMB, NES or other distributed file system protocols are well known in the art. It would have been obvious to one of ordinary skill in the art to use SMB, NES or other distributed file system protocols in order to define a series of commands that allow information to be passed between computers.

Regarding claim 20, Chi and McLain teach a system as in claim 1, in addition Chi teaches where said monitoring component comprises a monitor programmed to record certain information or types of information that flow across the isolated network as a result of the execution of the software program (col.6 lines 38-46; col.7 lines 2-12).

Regarding claim 21, Chi and McLain teach a system as in claim 1, in addition Chi teaches where said monitoring component comprises a monitor programmed to record at least one of certain operating system level or application level activities or types of activities that occur in real or emulated host computers as a result of the execution of the software program (col.6 lines 38-46; col.7 lines 2-12).

Regarding claim 22, Chi and McLain teach a system as in claim 2, in addition Chi teaches where said monitoring component comprises a monitor programmed to record at least certain activities or types of activities that occur in said server as a result of the execution of the software program (col.6 lines 38-46; col.7 lines 2-12).

Regarding claim 23, Chi and McLain teach a system as in claim 1, in addition Chi teaches where said monitoring component comprises at least one event handler programmed so as to obtain control when certain events or types of events occur (col.5 lines 15-20).

Regarding claim 24, Chi and McLain teaches a system as in claim 23, in addition Chi teaches where the certain events or types of events comprise at least one of creation of a new file in a filesystem, receipt of mail, an opening of mail, a posting of news, an opening of a new socket connection, an execution of a particular application, and an alteration of a system registry (col.3 lines 36-40; col.3 lines 49-52).

Regarding claim 25, Chi and McLain teach a system as in claim 1, in addition Chi teaches where said emulation component further comprises a system activity emulation component for emulating typical or specific activity on at least one of said isolated network and a real or emulated host computer (col.6 lines 38-46; col.7 lines 2-12).

Regarding claim 26, Chi and McLain teach a system as in claim 25, in addition Chi teaches where the typical or specific activity comprises at least one of sending mail, opening mail, opening or execution of a mail attachment, entry of keystrokes, issuing of user commands, execution of a particular application, rebooting a real or emulated host computer, restarting a real or emulated host computer, reinitialization of a real or emulated host computer, posting of news, participation in real-time messaging, and a transfer of files (col.3 lines 36-40; col.3 lines 49-52).

Claims 27-46 are rejected because of similar rationale outlined above.

4. Claim 3 rejected under 35 U.S.C. 103(a) as being unpatentable over Chi and McLain, and further in view of Chambers (US pat 5,398,196).

Regarding claim 3, Chi and McLain teach a system as in claim 1, but does not teach said emulation component is programmed so as to limit access by the software program to only certain resources. Chambers teaches said emulation component is programmed so as to limit access by the software program to only certain resources (col.7 line 63 thru col.8 line 27. It would have been obvious to one of ordinary skill in the art to combine Chi and McLain's apparatus for the detection and deletion of viruses with Chamber's teaching of limiting access to resources in order to protect and hide the resources from a virus, as well as concealing the presence of a monitor program away from the virus (Chambers col.8 lines 24-27).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tremayne M. Norris whose telephone number is (703) 305-8045. The examiner can normally be reached on M-F 7:30AM-5:00PM alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703) 305-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Tremayne Norris

July 12, 2004

Matthew B. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137